Use Cases in SAFETY Act Applications for Cybersecurity Technologies

Context for the Use Case: Review Process for SAFETY Act Applications

Applications for SAFETY Act protections are evaluated considering the criteria specified in the SAFETY Act. Several criteria focus on the *capability*, *effectiveness* and *utility* of the anti-terrorism technology (software, hardware, service or combination thereof) for which SAFETY Act protections are sought (referred to here as "the Technology").

A use cases approach is an effective technique for evaluating the Technology's capability, effectiveness, and utility, since a use case describes cybersecurity product functional requirements that will satisfy the user's business needs. There are many ways to developing use cases in SAFETY Act applications. They will vary from Applicant to Applicant, but the starting point for all applicants should be the same – asking the question about how the Technology can be employed to mitigate the risk of cyber terrorism. Use cases in SAFETY Act applications should demonstrate the potential for the Technology to be effective in countering potential acts of cyber terrorism.

Role of the National Institute of Standards (NIST) Cybersecurity Framework

The 2014 NIST Cybersecurity Framework (Framework) provides a useful model for describing cybersecurity products. It organizes and presents a mapping of essential cybersecurity functions, recognized best practices and standards employed by the Technology. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks. With DHS assistance, this general Framework has been implemented in more specific terms by most of the Critical Infrastructure sectors, and can be helpful in developing use cases for cybersecurity technologies to support SAFETY Act applications.

Use Case and Use Case Components

A use case is a methodology used in systems analysis to describe and organize system requirements. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to particular goals. In general, a use case for SAFETY Act applications should: 1) provide the functional context for SAFETY Act evaluators, 2) identify the typical requirements for features of the Technology, and 3) identify the applicable best practices and standards that meet the security requirements.

For applicants' convenience, we highlight below specific questions from the SAFETY Act Application Kit that will help an applicant develop use cases for their SAFETY Act applications:

- What is the Technology? (e.g. is it software, a service, a combination of both)
- What is it intended to do?
- What are its principal elements, systems, or components?
- How does it operate? (e.g. automated detection and/or isolation, manual monitoring)
- How, where and by who may it be utilized?
- If it is or incorporates a service, describe the actions, activities, planning, training, and/or expertise involved in its implementation?
- What specific potential does it have to counter cyber terrorism by deterring or mitigating an attack?

A typical use case will comprise the following information:

1. **Technology Capability**
    a. Scope: What does it do for the user?
    b. Components: What comprises the technology such as hardware, software, and human interaction?
        i. Security information and event management (SIEM) or log analysis software.
        ii. Industrial control system (ICS) equipment, such as remote terminal units (RTUs), programmable logic controllers (PLC), and relays, along with associated software and communications equipment. (e.g., radios, encryption software)
        iii. 'Bump-in-the-wire' devices for augmenting operational technology (OT) with encrypted communication and logging capabilities.
        iv. Software for collecting, analyzing, visualizing and storing operational control data. (e.g., historians, outage management systems, distribution management systems, human-machine interfaces)
        v. Products that ensure the integrity and accuracy of data collected from remote facilities.
    c. Functions – How does it operate?
        i. Interaction with other technologies or functions as a part of a broader system.
        ii. Maintenance required to function as intended including component repair and updating.
    d. Policies and Procedures
        i. Procurement process.
        ii. Use policies and user roles.
        iii. User training and management.
    e. Relevance – How does it guard against (or mitigate) cyber terrorism?

2. **Architecture**
    a. What does the network and/or software architecture diagram look like?
    b. What system and data security components are incorporated?

3. **Scenarios**
    a. What are some scenarios in which the Technology can prevent, detect, and/or mitigate a cyberattack?

4. **Requirements, Best Practices, Standards and Evidence**
    a. What are the technical requirements for mitigating defined risks associated with individual Technology components?
    b. What are the procedural requirements for the applicant's staff or end-users when using the Technology?
    c. What are the best practices employed to meet the intended Technology performance?
    d. What available evidence exists that the above requirements are being consistently met?

Examples of Use Case Components are contained in the Appendices.

Appendix A – Technology Capability

A use case includes a brief description of the Technology including an explanation of cyber threat intelligence lifecycle which is essential to developing a robust understanding of cybersecurity attacks.

Examples of a Technology description from a use case developed by NIST's National Cyber Security Center of Excellence (NCCoE):

"To improve the security of operational technology, energy companies need mechanisms to capture, transmit, analyze and store real-time or near-real-time data from ICS and related networking equipment. With such mechanisms in place, electric utility owners and operators can more readily detect anomalous conditions, take appropriate actions to remediate them, investigate the chain of events that led to the anomalies, and share findings with other energy companies. Obtaining real-time and near-real-time data from networks also has the benefit of helping to demonstrate compliance with information security standards."[1]

"Energy utilities rely on networked OT to control the generation, transmission and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of control system networks. A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots."[2]

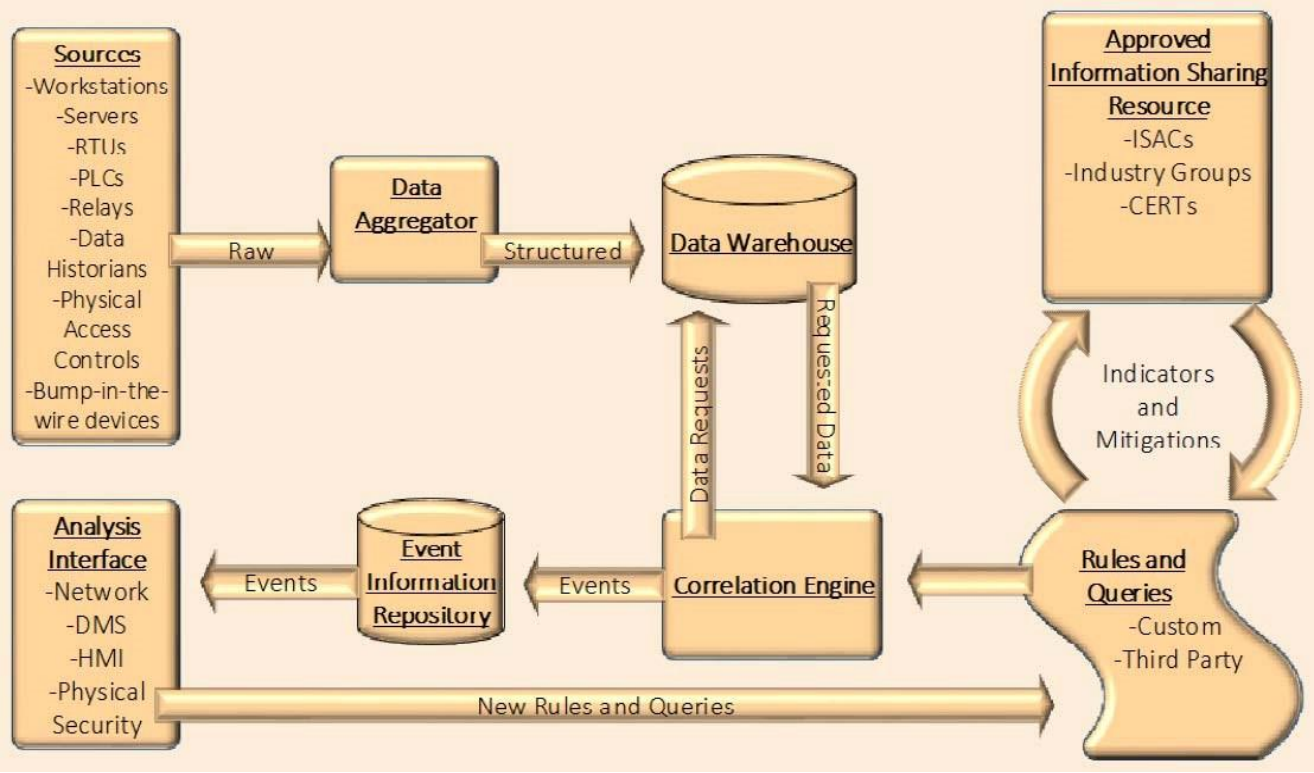
[1] *Situational Awareness: Secured Networked Infrastructure for the Energy Sector, Use Case, V.2* (Gaithersburg: National Cybersecurity Center of Excellence, National Institute of Standards and Technology, 15 November 2013)1.
[2] Ibid.

Appendix B - Technology Architecture

The architecture enables the applicant to illustrate the technical and management governance and identify foundational goals, characteristics, common roles and features, actors, and interfaces that are available across systems domains, while also illustrating cybersecurity cross-cutting concerns. The architecture may a single diagram or a series of diagrams if the Technology is comprised of multiple systems.

Ultimately, the architecture(s) must be well defined and documented. To be most useful, the architecture can be presented both in a narrative and graphically.

Below is an example from NIST NCCoE of High-Level Architecture.[3]



[3] Ibid., 4.

Appendix C – Scenarios

A scenario is a brief narrative explaining how the Technology is used, describing the actors, explaining the typical work flow of the Technology and demonstrating how the risk is mitigated.
An example from NIST's NCCoE is below:

"A dispatcher at an operations center sees that a relay has tripped at a substation and begins to investigate the cause. The dispatcher uses a single software interface that monitors system buses, displays an outage map, maps operational network connections to the bus and outage maps, and indexes logs from operational network devices and physical security devices. The dispatcher begins her investigation by querying network logs to determine whether any ICS devices received commands that might have caused the trip. If the answer is yes, then, using the same interface, she can automatically see logs of the most recent commands and network traffic sent to the relevant devices, allowing her to easily extend the investigation to internal systems and users who communicated with the suspect devices. The system may also be able to alert her to incidents of similar network traffic that were flagged as suspicious and shared by analysts at other power companies. If she finds that network traffic did not cause the trip, the dispatcher can check to see if there were any alerts from physical security devices that would imply a breach. This helps the dispatcher determine whether to send physical security personnel or a field technician to further investigate." [4]

[4] National Cybersecurity Center of Excellence, 1-2.

Appendix D – Requirements, Best Practices and Standards

The use case should employ a similar structure to the NIST Framework "Cybersecurity Framework Core" document.[5] Such structure relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience.

To demonstrate the real-world applicability of cybersecurity standards and best practices used to secure the Technology, an applicant should develop a table that maps the security characteristics of the Technology to applicable security best practices and standards. This table may include many relevant security characteristics and corresponding standards and best practices that are applicable to the Technology. Those presented standards and best practices are recommended to be hyperlinked to testing documentation or descriptions of procedures.

A modified example of such table from the NIST NCCoE use case is below:[6]

Example Characteristic		Cybersecurity Standards & Best Practices				Sector Specific Standards & Best Practices
Security Characteristics	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**NERC CIP v3/5**
device inventory	identification of all IT devices	Identify	Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	NIST SP 800-53 Rev. 4 CM-8	CIP-002-5 R1, CIP-010-5 R1

[5] *Cybersecurity Framework Core* (Gaithersburg: National Institute of Standards and Technology, 2014). Accessed August 11, 2016, at http://www.nist.gov/cyberframework/.

[6] Modified from *Situational Awareness: Secured Networked Infrastructure for the Energy Sector, Use Case, V.2* (Gaithersburg: National Cybersecurity Center of Excellence, National Institute of Standards and Technology, 15 November 2013), 8.

vulnerability management	mechanisms for identification of vulnerabilities and information sharing	Identify	Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16	CIP-003-5 R1, CIP004-5 R1, CIP-007-5 R1, CIP007-5 R2, CIP-007-5 R3, CIP007-5 R4, CIP-008-5 R1, CIP010-5 R2, CIP-010-5 R3
threat identification	mechanisms for identification	Identify	Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources ID.RA-3: Threats, both internal and external, are identified and documented	NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5, RA-3, PM-12, PM-16	CIP-004-5 R1, CIP007-5 R2, CIP-008-5 R1, CIP-010-5 R3